A Place of Greater Safety?

"An open society depends on individuals rediscovering the social value of privacy..."

UK CONFIDENTIAL

Edited by Charlie Edwards
and Catherine Fieschi

COLLECTION 25

DEMOS

Contributors:

Jonathan Bamford
Peter Bazalgette
Chris Bellamy
Peter Bradwell
Gareth Crossman
Simon Davies
Peter Fleischer
Niamh Gallagher
Tom Ilube
Markus Meissen
Perri 6
Charles Raab
Jeffrey Rosen
Robert Souhami
Zoe Williams
Marlene Winfield

First published in 2008

Magdalen House, 136 Tooley Street,
London, SE1 2TU, UK

ISBN 978-1-84180-192-6
Copy edited by Julie Pickard, London
Series design by modernactivity
Typeset by Chat Noir Design, Charente
Printed by Lecturis, Eindhoven

Set in Gotham Rounded
and Baskerville 10
Cover paper: Flora Gardenia
Text paper: Munken Premium White

UK CONFIDENTIAL

Edited by Charlie Edwards
and Catherine Fieschi

COLLECTION 25

DEMOS

Contents

REGULATING OUR PRIVATE LIVES IN AN OPEN SOCIETY

6 A place of greater safety? Information sharing and confidentiality

Perri 6, Chris Bellamy and Charles Raab

[Soldier guarding the National Convention] '… can we offer you an escort, Citizen Deputy, to a place of greater safety?'
'The grave,' Camille [Desmoulins] said. 'The grave.'[1]

In Britain and in several other countries in recent years, the pursuit of greater safety has informed policy in growing numbers of fields. Improving probabilities of detecting crimes, achieving early intervention to prevent crime and reduce criminality, providing greater reassurance to anxious citizens that everything possible is being done to protect children, preventing people with the most serious mental health problems becoming a danger to others, ensuring that future violent and sexual offenders are monitored carefully, managing anti-social behaviour and the like, are goals of increasing importance to policy makers. Indeed, systematic risk assessment is now required in many fields, including those where people are considered to be a danger to themselves, as well as those where they present risks to the wider public.

The language of risk is now ubiquitous. In care for frail older people, for example, 'risk assessment', and not just the assessment of needs, is now routine in order to identify those who are susceptible to falls. In British public policy, the key to promoting safety is now the encouragement, through legislation, national policy guidance and a plethora of model protocols, of the sharing of personal information between agencies providing frontline services.

At first sight, it might seem surprising that information sharing should be thought the highway to safety. For sharing information carries no guarantee of its being acted on, still less of its being acted on appropriately. Indeed, for all that it has become

commonplace to describe the horrible death of Victoria Climbié as a failure of information sharing, this is factually incorrect. In her wretched case, the relevant information was shared about Victoria's injuries, but in a form that failed to alert those who should have been alerted to her plight, or to draw the correct inferences from the information.

Similarly in the case of Ian Huntley, who killed two schoolgirls in the Cambridgeshire village of Soham. Information sharing may well have had a lesser significance for his employment as that village's school caretaker than is commonly thought. Information was not retained in the intelligence systems of Humberside police because the allegations against him were insufficiently evidenced to enable charges to be laid – let alone for the Crown Prosecution Service to advise that any be taken forward. Most of the cases did not concern children below the age of consent.

Nevertheless, ministers and many policy advisers remain firmly of the view that the sharing of more information about those classified as either at risk or else as presenting a risk will provide the critical infrastructure for more effective public protection. A central aspiration in policy has been, therefore, to remove blockages to the sharing of information. Chief among the barriers to information sharing, policy makers assume, is the widespread misunderstanding of the Data Protection Act 1998, which, when correctly understood, by no means prevents sharing where it would generally be warranted on public interest grounds.

Ministers' public statements typically present the issue of information sharing as one to do with finding a better 'balance' between effective inter-agency working and client confidentiality. In fact decisions about information are rarely matters of 'balance' at all. A decision whether or not to share information is taken precisely at the point where, by definition, no public service holds all the information that might be made available. That means decisions involved in sharing enough information to judge whether pooling it would be wise commit the service to one course of action. These are in fact dilemmas requiring a choice and a judgement, not problems calling for some judicious mix of sharing and confidentiality.

The dilemma is this. Any decision rule that would err on the side of avoiding the risks associated with not sharing information in a particular case, will sooner or later err on the side of sharing information – and perhaps of acting with inappropriately draconian

intrusiveness – when in fact the person is not at risk. Indeed, it was only a decade before Victoria Climbié's case that social workers were excoriated for taking children into care in Orkney and Cleveland as a result of sharing information that had been wrongly interpreted to indicate high risk.[2]

The call for greater information sharing is not confined to contexts such as child protection and mental health where it may be shared on a case-by-case basis. The Labour government's programme also calls for greater 'bulk' sharing, or routine access by public service agencies to at least some of each other's information about clients – for example to check entitlements to service, to complete risk assessments or to cross-match records to detect possible cases of fraud.

Four public service contexts

It can therefore be said with some confidence that questions about information sharing between public services constitute some of the most difficult and urgent privacy challenges of this decade. Yet safeguarding privacy, understood as a human right, is not the only, or even the most pressing, reason for which we might care about confidentiality.

Confidentiality is often a critical means to the pursuit of service goals. For example in fields such as mental health, substance abuse and sexually transmitted infections, a strict confidentiality regime is necessary to persuade clients to present themselves and to be candid with professionals. In many human services, confidentiality protection helps to prevent stigma and to preserve employment and social relationships that may be critical to achieving service goals. In still other cases, agencies may worry that sharing information may lead another agency to take inappropriate action because they may fail to appreciate its full and proper context.

Sharing information often presents the greatest difficulties of principle when the decision to be made concerns sharing between services with different types of purpose. Table 6.1 shows some of the basic types of services between which sharing often raises the most fundamental operational problems, and sometimes ones of principle, too.

Table 6.1 **Four pure types of service context**

	Universal distribution	Selective distribution
Public benefit	**A** Personal direct taxes Social insurance payments Driving license registration Citizen registration	**C** Probation Youth offending Policing MAPPAs and CRB
Individual benefit	**B** Education General health services Social insurance benefits	**D** Child protection Services for older people Specialist health services Drug/alcohol abuse services

The problem is that services with different purposes have very different conceptions of their stewardship of client information, and these conceptions cause them to manage information in very different ways. We typically expect type A services to gather most information from clients themselves and to take information from other services only under specific legal powers. Type B services have generally been expected to keep information within their own 'family' or related health or education services and tend to be subject to professional protocols that codify duties towards clients.

Type C services have generally been required to show good grounds before requiring information from other services and to keep intelligence to themselves, especially where the information is 'soft'. Type D services may also deal in soft information but will tend to do so under professional confidentiality codes. In recent years, however, policy imperatives to share information, and especially to lower the thresholds for sharing with type C services, have blurred many of the boundaries between cells in Table 6.1. In the process, they have exacerbated the dilemma between risks associated with information sharing and confidentiality.

In response, the government has looked for *general* solutions to this policy problem. In 2000/01, the then Performance and Innovation Unit, now the Prime Minister's Strategy Unit, was commissioned to produce a report that finally appeared in 2002, entitled *Privacy and Data Sharing: The way forward for public services*.[3] Its recommendations for new legislation to create a general power for information sharing found little favour with government lawyers. When responsibility transferred to the Department for

Constitutional Affairs (now the Ministry of Justice) the department issued new legal guidance in November 2003, the burden of which was that existing powers provided all the cover required for any sensible sharing. It recommended that locally agreed protocols would suffice to govern information sharing in specific cases of inter-agency working. However, continuing scandals, which were widely attributed to information-sharing failures, led ministers to call for new initiatives to promote more extensive information sharing.

In late 2006, a 'vision statement' was published, promising much freer information flows but without providing much detail. Responsibility for publishing the statement was left to a cabinet committee, MISC 31. In the meantime, however, government brought forward new legislation creating information-sharing powers and duties to combat serious and organised crime, along with other proposals, including a children's database, a population register to underpin the national identity card scheme, a range of early years and even prenatal interventions to target those believed most likely, on the basis of long-range predictive modelling, to present future risks.

There are problems with both these approaches. The search for a single, general and overarching principle that could be set out in legislation seems likely to prove misguided, and it would, in any case, have to leave wide scope for discretion. The thresholds of probability and the severity of risk that would lead to information sharing in child protection cases are surely very different from those that are appropriate in detection of benefit fraud. In fields where willingness to present and to be candid with professionals is critical, disclosure rules have to be rather different from those in fields where financial entitlements are at stake.

In all these fields, decisions about sharing and confidentiality involve judgements about which staff within which agencies have a legitimate 'need to know' a specific piece of information, or to claim routine access to types of information. Such judgements also depend on how much, of which types of information, are proportionate to the risks presented by cases in different fields. However, these judgements cannot be made using algorithms, ie rules taking the form, 'if these circumstances obtain, always share [or do not share] this information with these other services'. No such algorithms are available, even for decisions about bulk

sharing. Instead, claims about 'need to know' and 'proportionality' must be justified on the basis of arguable principle.

Dealing with the risks of risk assessments

'Risk assessment' for decisions of this kind, undertaken appropriately, must be *symmetrical*. That is to say, it should consider equally the risks arising both from sharing and from not sharing. Unfortunately, however, too much of the guidance presently given to practitioners encourages them to consider principally the risks arising from not sharing, on the assumption that these risks are generally worse. We argue instead that risk assessment should be conceived in terms of appraising the risks to the whole range of service outcomes including those arising from breaches of confidentiality, on the one hand, and the risks associated with not sharing, on the other.

Policy makers should also think about the ways public services could cultivate the skills and institutional capabilities for making and supporting these kinds of judgements. This is a very different policy problem from designing rules, and is a long way from resorting to simplistic calls for thresholds of probability and severity to be relaxed each time there is some service failure that may seem, at first glance, to be something to do with information sharing, or indeed, raising them, as was the response to the Orkney and Cleveland scandals.

Some professionals will, quite understandably, demand explicit rules to follow rather than be required to exercise personal judgement. This is particularly the case if they have reason to fear that, should conscientious and competent decisions turn out badly, politicians will expose frontline workers to personal blame and obloquy.

To illustrate this point, the cases of Victoria Climbié in Haringey and Caleb Ness in Edinburgh provide a powerful contrast. In the Climbié case, it was the frontline social worker, Ms Lisa Arthurworrey, who bore the brunt of the blame for the mistaken judgements made in that case, and she was placed on the register of those who should not be permitted to work with children. Yet there is evidence that she received totally inadequate training, support and guidance from her managers, and was given a case load beyond her capacity to cope. By contrast, for the errors

made by social services in the Caleb Ness case, Les McKeown, the Director of Social Work in Edinburgh, resigned. The differences in the degree to which blame was individualised for catastrophic decisions will have proved very important in signalling to professionals in England and Scotland the need for defensive practice in relation to sharing information.

However, what constitutes practice that is defensible against blame is difficult for many professionals to call. There is no shortage of guidance for frontline staff on the legal aspects of information sharing. In almost every field of public services, central government bodies, professional institutes and local bodies have issued fat volumes of notes on the meaning of all relevant legal doctrines, from the principle of the paramountcy of the welfare of the child in child protection, through the legal powers of inspection for fraud detection officers, to the meaning of every relevant clause of the Data Protection Act, of the central concepts of the common law of confidentiality, of Article 8 of the Human Rights Act and much else besides. Locally agreed protocols on information sharing can run to over a hundred pages. In a large-scale study we conducted recently, we found to no one's great surprise that few professionals regularly consult any of these documents.

If there is a need for any more central policy intervention, it should surely not be designed to provide yet more guidance on the law, unless it be by way of handy summary. Rather, the focus should be on building competence through training, rather than producing yet more documents to clutter up the web. This training should be in the skills of symmetrical risk assessment, and the risks should be more holistically conceived. If there is to be more guidance, it should be aimed at managers rather than professionals, and should make the case for a less individualised and blame-oriented culture of management, and discuss practices that can most constructively be adopted when cases do go wrong, as inevitably they sometimes will, whatever decision norms are adopted. Most important, politicians should consider, before they reach for the easy option of blaming the frontline staffer or manager, what the consequences of devolving blame to lower levels may be for future decision making and public services in the relevant field.

The information sharing issue also raises some more general lessons about joined-up government. 'Joined-up' public services means, in practice, the joining up of purposes for which our

personal information is collected, used and disclosed. In many cases, of course, this can be done sensibly and without contention. Few would doubt that any medical professional should, and in many cases commonly now would, alert other services if they saw evidence of neglect or violence in a child that was unlikely to be accidental.

It is also important to recognise, however, that we run great risks of undermining public services – independently of issues to do with privacy in its narrow sense – if we simply declare that all such services are obliged to use personal information they collect for their own purposes to further the goals of all public services, without exercise of judgement. Not only will the obvious imperatives of ensuring that clients and patients are willing to present and talk candidly about personal and social problems be undermined, but an issue of even more fundamental importance is at stake. Public trust in public services depends in no small measure on the degree to which people can understand and recognise the goals of these services as *delimited*, and recognise purposes for which they will use personal information as legitimately related to the core business of the service. As goals and purposes begin to sprawl and swell, their transparency, intelligibility and legitimacy is undermined.

At the heart of the issue there is a fundamental question about the causal relationships between opposing risks. At one meeting in Westminster not many years ago, we heard one child protection professional claim that if there were more cases of children being taken wrongly into care on the basis of sharing information that was over-interpreted, then that would be a sign that things were moving in the right direction, because it would indicate that fewer children who really are at risk are being missed: more cases of 'false-positive' judgement errors would be a price worth paying to save more children from abuse and neglect. This professional's emotional engagement with the plight of abused children cannot be faulted, but the reasoning in that remark is open to strong objection.

It simply does not follow that, because we are sharing even to excess and over-interpreting, we must consequently be guilty of fewer cases of insufficient sharing and under-interpretation of information. We could be misdirecting our efforts entirely. But, further, it is not at all obvious that the long-term cost of false-positive judgement errors would be a price worth paying for such an outcome. A system that routinely runs the risk of such errors will

not indefinitely sustain public trust, as the legacy of the Orkney cases and the 'satanic ritual abuse' panics of 20 years ago showed. Politicians who call for 'more information sharing' and 'greater safety', and think that easy banalities about 'balance' and 'safeguards' cope sufficiently with the opposite risks, should think again.

Perri 6 is Professor of Social Policy, Nottingham Trent University; Chris Bellamy is Professor of Public Administration, Nottingham Trent University; and Charles Raab is Professor of Government, University of Edinburgh.

Notes

1 H Mantel, *A Place of Greater Safety* (Harmondsworth: Penguin, 1992).

2 It should be said that controversy continued for some time afterwards about the facts of some of those cases.

3 Performance and Innovation Unit, *Privacy and Data Sharing: The way forward for public services* (London: Cabinet Office, 2002), available at www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/strategy/piu-data.pdf (accessed 3 Mar 2008).